Chapter 42 - Counterintelligence

4201 Purpose

This chapter provides general guidance for servicing security officers, security contacts, and employees concerning the Department's counterintelligence (CI) policy, procedure, and activities. Counterintelligence terms are defined in Appendix A, Glossary of Security Acronyms and Terms.

4202 Authority

The provisions of this chapter comply with the applicable Executive Orders, public laws, statutes, directives, and regulations issued within the Federal Government, which pertain to counterintelligence programs and activities in the Department. In accordance with Department Organization Order 20-6, the Director for Security will implement a Counterintelligence program. To ensure the existence of a comprehensive CI program and the consistent application of CI policies and procedures, CI efforts will be established at the Department and operating unit levels. Pertinent references include:

- Executive Order 12333, United States Intelligence Activities, December 4, 1981.
- PDD/NSC-12, Security Awareness and Reporting of Foreign Contacts, August 5, 1993.
- PDD/NSC-24, U.S. Counterintelligence Effectiveness, May 3, 1994.
- PDD-39, U.S. Policy on Counterterrorism, January 24, 1997.
- PDD-62, Combating Terrorism, May 22, 1998.
- PD/NSC-63, Critical Infrastructure Protection, May 22, 1998.
- Director of Central Intelligence Directive 1/7, Security Controls on the Dissemination of Intelligence Information (June 30, 1998).
- Security Policy Board Issuance 6-97, National TSCM Policy, September 16, 1997.
- Gathering, transmitting, or losing defense information (18 U.S.C. § 793).
- Gathering or delivering defense information to aid foreign government (18 U.S.C. § 794).
- Disclosure of classified information (18 U.S.C. § 798).
- Economic espionage (18 U.S.C. § 1831).
- Theft of trade secrets (18 U.S.C. § 1832).
- Coordination of counterintelligence activities (50 U.S.C. § 402a.).
- Offenses concerning control of subversive activities (50 U.S.C. § 783).

4203 Application

This chapter of the Security Manual implements the Departmental Counterintelligence Program **(**DCIP). The principal aim of the DCIP is the identification and exploitation, or neutralization, of adversarial, foreign collection threats targeting departmental persons, facilities, information, or activities. Unless specifically noted otherwise in this chapter, all previous departmental counter-intelligence guidance is hereby rescinded. The provisions of the DCIP apply to all Departmental organizations and personnel, including contractors, experts and consultants, guest workers, and research associates/scientists who have on-going, official association or who work directly on activities, projects or programs of the Department, hereinafter referred to collectively as "DOC persons."

4204 The Threat

In the decade since the demise of the Soviet Union, radical changes have occurred in the sources and nature of the espionage threat directed against the United States. The massive targeting of our military-industrial complex has been significantly reduced, replaced with patient and long-term collection strategies against our scientific and technological bases. Even more pervasive is the persistent targeting of the U.S. economy. Adversaries ranging from small emerging nations to older established nations striving to restructure aging economies have increased the overall espionage threat to levels exceeding those of the Cold-War era. The Department of Commerce resides at the center of the U.S. economy. Furthermore, the Department is the principal U.S. Government policy developer and enforcement arm for the control of critical technologies. Together, these two roles make the Department a prime target of adversaries seeking to compromise economic data and strategies and to acquire advanced U.S. technologies.

4205 Counterintelligence Policy

A. The DCIP resides in the Office of Security based on DOO 20-6, Director for Security. As the senior Departmental CI Official (DCIO), the Director for Security provides executive leadership and oversight to the DCIP. The DCIO serves as the principal department staff member representing the Department to all external counterintelligence organizations, boards, committees, and councils. Delegation of this function is at the discretion of the DCIO.

B. The DCIP consists of several sub-functions. These functions are listed below and their definitions can be found in Appendix A, Glossary of Security Acronyms and Terms.

1. Counterintelligence inquiries.

2. Threat Analyses, Notification, and Education.

3. Counterintelligence Vulnerability Assessments.

4. Technical Surveillance Countermeasures.

5. Foreign Contact Reporting.

6. International Treaty/Agreement Support.

7. Counterintelligence Community Liaison.

8. Counterintelligence Support to Critical Infrastructure Activities.

9. Counterintelligence Support to Information Systems Protection Operations.

10. Counterintelligence Support to Counterterrorism.

11. Counterintelligence Support to Other programs.

D. Program Coordination.

1. The DCIO ensures that departmental CI activities are coordinated with appropriate elements of the U.S. Intelligence Community.

2. On matters involving departmental activities in foreign countries, the DCIO ensures that CI activities are coordinated with the CI element of the U.S. State Department's Diplomatic Security Service.

3. All legal matters pertaining to counterintelligence will be thoroughly coordinated with the Department's Office of the General Counsel.

E. Policy Promulgation and Applicability.

1. DCIP policy may be promulgated only by the DCIO. All operating units will develop internal procedures implementing DCIP policy. Procedures developed by the operating units will be reviewed and approved by the DCIO prior to implementation.

2. The provisions of the DCIP apply to all departmental organizations and personnel, including contractors, temporary/part-time employees, guest researchers/scientists, and consultants. The term "DOC person" means any one or all of the above categories of personnel.

4206 Counterintelligence Inquiries

A. General.

1. Procedures contained in this chapter are intended to provide guidance to servicing security officers, operating unit security contacts, and departmental personnel at large. In certain instances, more detailed guidance may be provided to servicing security officers and security contacts on specific issues or activities.

2. Unforeseen or special circumstances may necessitate the alteration of these procedures without advance notice.

3. Requests for exception to these procedures will be addressed, in writing, to the Office of Security. Requests will be appropriately classified and will include:

a. A statement identifying the procedure to which the exception is requested;

b. A statement justifying the request; and

c. The date when the exception is needed and the anticipated date when full compliance with the procedure will occur.

Note: An exception to this policy is intended to provide the requestor with the ability to continue conducting business while concurrently developing and implementing a solution that provides full compliance with departmental policy. *Exceptions to CI policy are only temporary*.

B. Counterintelligence Inquiries.

1. A counterintelligence inquiry will be initiated when one of the following circumstances exists:

a. A Department of Commerce person is known or suspected of having contact with a member of a foreign intelligence service.

b. A Department of Commerce person is known or suspected of having contact with a citizen of a country that has been designated as a CI-sensitive country. The CI-sensitive country list is available from the Counterintelligence Branch of the Office of Security.

c. A Department of Commerce person is known or suspected of having traveled to a CI-sensitive country and has failed to report the travel.

d. An incident occurs that involves a Department of Commerce person, and/or occurs within a departmental facility or installation, in which there are indications of possible espionage, sabotage, subversion, or terrorism or support any of the foregoing.

e. When information exists that a Department of Commerce person has not complied with this policy.

f. At the request of an external, authorized investigative organization, such as the Federal Bureau of Investigation (FBI).

g. At the direction of the Secretary, Deputy Secretary, Chief of Staff, or the DCIO.

2. Department of Commerce personnel who are aware of a circumstance as described in paragraph 4205 B.1 a. through e. above are required to report the matter to their security contact, servicing security officer, or directly to the CIPB. Without exception, all reports in accordance with this requirement will be made either in person or via secure means only. Failure to report violations or non-compliance with this policy constitutes a violation of policy.

NOTE: The Incident Reporting Information Management System (IRIMS) will not be used to report incidents of possible CI interest.

3. Only members of the CI Program Branch will conduct CI inquiries, unless directed otherwise by the DCIO.

4. The nature of CI inquiries requires extreme discretion both in the interest of the privacy of the subject as well as in the interest of national security. The Director for Security will approve all requests for access to CI investigative files by persons or organizations external to the CIPB. Disputes will be referred through the supervisory chain to the DCIO for resolution. Requests for access to CI files must be in writing with a justification for access.

5. Adverse information about an employee developed during the course of a CI inquiry will be reported to the Office of Security.

6. Information developed during the course of a CI inquiry, which meets the reporting threshold reflected in 50 U.S.C. § 402 (a), will be referred to the FBI.

7. During the conduct of a CI inquiry, CI Program Branch members are authorized to:

a. Administer oaths and interview subjects, witnesses, and sources for information;

b. Access, review, and copy an employee's personnel and security files or other departmental records relevant to the inquiry;

c. Conduct local record checks and other required external inquiries;

d. Implement technical CI activities when such actions will enhance the investigative process, or when such actions are necessary to confirm or refute information which is critical to the inquiry; and

e. Initiate non-alerting processes for acquiring, reviewing, downloading, and/or copying an information system's data and/or software which is key to the inquiry, or which has been used, is being used, or will be used by personnel that may be a subject, witness, or source of the inquiry.

8. All CI inquiries will result in one of the following conclusions:

a. The matter is referred for further investigation;

b. The Office of Security resolves the issue through the personnel security process;

c. Formal action is taken against the subject of the inquiry; or

d. The matter is appropriately reported and the case is closed pending additional information that might support further inquiries or other action.

4207 Threat Analysis, Notification, and Awareness

A. Threat Analysis and Notification.

1. The Counterintelligence Program Branch is responsible for maintaining current information about known or potential threats to Departmental persons, facilities, information, or activities

stemming from the activities of foreign intelligence services, international industrial espionage, or domestic or international terrorism.

2. The CI Program Branch is not specifically responsible for threat analysis with regard to criminal activity, workplace violence issues, or cyber threats, but can assist in such determinations. Threat information outside the scope of the CI Program Branch will be immediately referred to the appropriate Office of Security program manager or to the Chief Information Officer. [Note: Threat analyses supporting Secretarial/Deputy Secretarial travel will include information on any issue that may pose a threat to the safety of the party.]

3. The CI Program Branch will ensure proper and timely dissemination of threat information to all elements within the Department. Notification of threat information will be made to the servicing security officer, who will then be responsible for dissemination to the appropriate security contacts.

a. Unclassified threat information is routinely disseminated by the CI Program Branch to servicing security officers via e-mail or by other secure means if the information is sensitive and requires increased protection.

b. Classified threat information will be made available to servicing security officers via secure voice, secure facsimile, or other secure automated information systems if available.

c. Threat studies conducted for Secretarial/Deputy Secretary travel will be provided to the Executive Protection detail leader, or to an individual designated by the Director for Security.

d. Threat analysis support can be provided by the CI Program Branch upon request by either the servicing security officer or the operating unit's security contact. Requests will be made in writing through the servicing security officer to the Office of Security, and will be classified appropriately. The location or function and the available threat information will dictate the classification of the analysis. The CI Program Branch will make all attempts to meet the classification needs requested, but cannot guarantee that the final product will be unclassified or classified at any particular level. Each request will identify what is needed (formal briefing, informal discussion, hard-copy report, educational awareness information, etc.), why it is needed, date required, and the intended audience.

e. The Director for Security will make a determination as to the priority of the request based on program sensitivity, existing tasks, and resource availability. If a request cannot be met, the requestor will be contacted and the issue(s) resolved.

f. The CI Program Branch can develop or facilitate access to material for threat awareness educational purposes.

g. Requestors should allow at least a 30-day lead-time when requesting formal briefings or final written studies.

B. Counterintelligence Awareness.

1. The success of the DCIP and departmental security efforts depends upon the counterintelligence awareness of all employees. This includes the threats they could face, the precautions they should practice in view of any potential threats, and departmental policy governing their actions.

2. Employees who fall into one or more of the categories indicated below will attend a CI-awareness briefing on an annual basis.

a. Employees with access to classified national security information.

b. Employees with access to data or technologies that are known or considered to be an interest of a Foreign Intelligence Services (FIS).

c. Employees who have on-going contact with a representative of a designated CI-sensitive country.

d. Employees who travel to designated CI-sensitive countries. [Note: Defensive travel briefings, which are required of certain employees for travel to select countries, *do not* qualify as an individual's annual CI awareness session.]

e. Servicing security officers and security contacts are responsible for conducting or ensuring that CI awareness sessions are conducted. A representative of the CIPB may be available to attend these sessions as the DCIP spokesperson, time and travel funds permitting.

3. CI awareness sessions should be conducted multiple times during the year to ensure that all employees have ample opportunity to attend. The CI Program Branch will provide guidance on the substance of these sessions as well as assistance in obtaining materials for use during these sessions. CI awareness sessions may be conducted at the classified or unclassified levels, or both may be done in separate sessions. The servicing security officer or security contact will

make this determination in consideration of the clearance levels of the supported employee population, the availability of an appropriate facility, and the awareness needs of the employees.

4208 Counterintelligence Vulnerability Assessments

A. A Counterintelligence Vulnerability Assessment (CIVA) is a thorough analysis of a Departmental facility, system, property, activity, or specified information holding to determine the degree to which the entity is susceptible to an identified threat. Unless there is an identified threat, vulnerability assessments are not conducted. The CIVA is typically a follow-on service, conducted after a threat analysis has identified an actual threat condition. The comparison between the threat condition and actual day-to-day circumstances provides the analyst with the necessary insight that will allow a sound judgment to be made regarding the possible nature and degree of harm that a threat condition can inflict. An inherent part of the CIVA is the development of recommendations on the employment of countermeasures necessary to counter identified vulnerabilities.

B. A CIVA may be conducted based on a request from a servicing security officer or security contact, or when the DCIO determines that a sufficient threat potential exists that warrants the conduct of a vulnerability assessment.

C. The servicing security officer or security contact will request the conduct of a CIVA, in writing, to the Office of Security. The request will contain basic information identifying the location, activity, or facility on which the CIVA will be conducted, the nature of the threat (if unknown to the CI Program Branch), and the timeframe in which the CIVA is to be conducted. The Director for Security will assess the request in terms of priority, available/required resources, and the timeframe in which the service is requested.

D. The composition of the CIVA team will vary according to the entity being assessed. Typically, the team will be headed by a CI specialist together with an analyst, a member of the requesting organization's security office, and subject matter experts from the location, activity, or facility being assessed. Subject matter experts from other security disciplines within Office of Security may also be called upon to participate.

E. A CIVA is conducted at the location, facility, or activity of the suspected vulnerability. The assessment may include multiple facilities, locations, or activities. The team members will require complete access to all data regarding the subject as well as access to personnel employed at, or engaged in, the subject. Special access must be identified in the request for the service, if required. Team members will require dedicated workspace, telephone/facsimile support, and information systems support in the identified facility, location, etc.

F. The CIVA team leader will initiate the assessment with an entrance briefing to the managers of the activity or facility being assessed. The host servicing security officer or security contact should identify the attendees for the initial briefing. The entrance briefing will cover the purpose of the assessment, protocols and procedures, support required from the host organization, anticipated timeframe for the conduct of the CIVA, and anticipated interruptions to the work force, if any. At the conclusion of the CIVA on-site period, the team leader will conduct an exit briefing and provide the findings that have been determined up to that time.

G. The final CIVA product will be provided to the requestor within four to six weeks from the conclusion of the on-site period.

4209 Technical Surveillance Countermeasures

A. In accordance with national policy governing technical surveillance countermeasures (TSCM) as issued by the U.S. Security Policy Board (SPB), the Office of Security will develop and implement a departmental TSCM program. TSCM is an inherent function of counterintelligence, therefore the responsibility for the TSCM activities will reside within the CI Program Branch. All matters pertaining to the conduct of TSCM activities will be directed by the Director for Security, consistent with SPB TSCM Procedural Guides 1 through 3.

B. The Director for Security will ensure that a TSCM capability exists which can:

1. Conduct physical, electronic, and visual search techniques necessary to identify and protect Departmental persons, facilities, information, or activities that are vulnerable, through design or circumstance, to hostile technical surveillance activities;

2. Acquire and employ TSCM technologies, techniques, methods, and measures to identify and neutralize hostile technical surveillance activities;

3. Collect, analyze, and disseminate data regarding the technical surveillance threat to the Department, its persons, facilities, information, or activities;

4. Provide state-of-the-art support by ensuring that all TSCM personnel are accredited, and that the individuals receive continuing, advanced training necessary to maintain the level of technical expertise prescribed by TSCM Procedural Guides 1 through 3;

5. Review and/or develop practices and procedures for routine departmental functions that will allow departmental persons to ensure their activities are in compliance with this chapter; and

6. Provide recommendations to the DCIO concerning significant issues that involve either the conduct of a TSCM service, technical vulnerabilities to the Department, or the discovery of an unauthorized device.

C. Request Procedures.

1. All requests for TSCM support will be addressed to the Office of Security and classified at the Confidential level at a minimum.

NOTICE: Advance coordination may be made verbally, but only via secure means. When requesting or coordinating a TSCM service, requestors will not use any communication medium that is located within the room/area that is to be the subject of the TSCM service.

2. As a minimum, the request must identify:

a. The specific room/area to be serviced;

b. The function of the facility, the nature of, or the cause for, the request;

c. The name of the point of contact; and

d. The time frame in which the service is desired.

3. The workload and availability of assets of the CI Program Branch may necessitate the service being conducted at a time other than when originally requested.

D. Requirements.

1. A TSCM service will be performed at least annually in any room, office, suite, facility, etc., storing or processing Sensitive Compartmented Information (SCI) or in which SCI discussions occur.

2. A TSCM service will be conducted in all SCI facilities (SCIF) when there is a suspected compromise of information or when unauthorized personnel are left unattended within the perimeter of the SCIF.

3. Annual TSCM services will be conducted in all offices in which routine Top Secret discussions occur.

4. Annual TSCM services will be conducted in offices or areas that are routinely used to process information or to discuss information which:

a. Addresses sensitive aspects of controlled U.S. technology; or

b. Details a U.S. position on trade, treaty negotiations, or sensitive aspects of current treaties or trade agreements.

5. A TSCM service will be conducted due to threat conditions when determined by the Director for Security.

E. In Department of Commerce facilities, TSCM services will be coordinated by the CI Program Branch. Any exceptions to this policy will be approved by the Director for Security, in writing, prior to conducting the service. Requests for exceptions will be forwarded to the Office of Security at least 30 days prior to the proposed date of service.

4210 Foreign Contacts

A. The principal concern of most CI programs is espionage against the host organization. The Department's mission, responsibilities, and activities often demand close and sometimes-continual contact with foreign nationals. The DCIP seeks to apply national, Departmental, and personal safeguards to the conduct of this business, not to restrict it. Adversarial foreign intelligence services (FIS) also understand very well the nature of the Department's mission. The enormous degree of exposure that departmental persons have with foreign nationals creates vulnerabilities for the Department and opportunities for a foreign intelligence service. The routine contacts are excellent venues for FIS officers to conduct the spotting and assessing, necessary in identifying the right individual for recruitment.

B. Contact with foreign nationals can occur in several ways. The most common are the following.

1. Purposeful contact due to legitimate business reasons, whether inside or outside of the United States.

2. Incidental contact whether in or outside of the United States. The various types of incidental contacts are too numerous to list. Generally, incidental contact is one in which the departmental person did not initiate the contact, there is no departmental purpose to the contact, and no follow-up meeting was suggested by the other party. Although seemingly innocent, incidental contact has been the start of many espionage cases; hence, it is always in

the best interest of the departmental person to maintain a constant vigilance of the actions occurring around them as well as their own actions in regard to contact with foreign nationals.

C. PDD/NSC-12, Security Awareness and Reporting of Foreign Contacts, Paragraph 6.1BI, requires the reporting of contacts with foreign nationals as well as the maintaining of records about these contacts. Departmental procedures for reporting foreign contacts are contained in Chapter 17, National Security Information Policies.

D. Office of Security interest in foreign contacts is twofold. Certain countries have been designated as CI-sensitive and certain subject matter or technology has been designated as being of interest to certain foreign intelligence services.

E. Foreign contact reporting is accomplished through the Department's Personnel Assurance Program (see Section II, Personnel Security). Arrangements between the CI Program Branch and the Personnel Security Officer serve as the means by which information concerning foreign contacts of interest is forwarded to the Branch. Servicing security officers, security contacts, or other individuals are authorized to report directly to the CI Program Branch. In such cases, the CI Program Branch will forward information to the Personnel Security Officer.

4211 International Treaty/Agreement Support

A. International treaties and agreements can provide a foreign intelligence service with excellent, overt opportunities to operate within the United States. Typically, these arrangements provide sanctioned, foreign access to critical government facilities and/or to critical U.S. industries/technologies. Unfortunately, some international agreements have been the basis for compromise of sensitive and classified information and activities. The key to this critical failure can be attributed to one recurring theme, improper consideration of CI concerns during the planning and, in particular, the implementation phases of international treaties and agreements.

B. Departmental persons engaged in any aspect of international treaties or agreements are required to report their involvement to the CI Program Branch. The Branch is required to assess the threats to the Department, while ensuring that proper safeguards are implemented and are consistent with national security objectives and concerns.

C. The CI Program Branch will serve as the departmental liaison to external organizations for all counterintelligence matters, with regard to the Department's involvement in international treaties or agreements.

4212 Counterintelligence Community Liaison

A. Maintaining liaison with counterparts in the Federal Government, states/communities, and private industry is essential to the DCIP's success. Active liaison by servicing security officers with their local law enforcement offices and with supporting FBI offices is encouraged.

B. The Counterintelligence Program Branch serves as the principal departmental liaison to Federal counterintelligence elements.

C. All employees will immediately notify the CI Program Branch if they have been contacted by any organization external to the Department, whether Federal or state, for any issue relating to counterintelligence, counterterrorism, contact with a non-U.S. citizen, or threats to departmental facilities, persons, property, or activities.

4213 Counterintelligence Support to Critical Infrastructure Protection

A. PD/NSC-63, Critical Infrastructure Protection, Paragraph 6.1BI, establishes the broad policy and the organizational framework for addressing protection of the country's critical infrastructures such as telecommunications, banking and finance, energy, transportation, and essential government services.

B. The Chief Information Officer (CIO) serves as the Department's program office for Critical Infrastructure Protection (CIP).

C. The CI Program Branch support to the CIP consists of the following activities:

1. Threat analyses.

2. Vulnerability assessments.

3. CI inquiries.

4. Technical CI support.

D. The CI Program Branch's support to the CIP can be initiated at the request of the CIP program office or internally initiated by the CIPB based on the receipt of credible threat information.

E. The CIP program office can request support by contacting the CI Program Branch to discuss support requirements. Once agreement is reached, the CIP program office will submit a written request to the Office of Security.

4214 Counterterrorism

A. PDD-39, U.S. Policy on Counterterrorism, and PDD-62, Combating Terrorism, Paragraph 6.1BI, establish and define U.S. policy with regard to combating terrorism. Terrorism is defined as "The calculated use of violence or threat of violence to inculcate fear; intended to coerce or to intimidate governments or societies in the pursuit of goals that are generally political, religious, or ideological."

B. Combating terrorism is divided into two basic sub-components, antiterrorism (AT) and counterterrorism (CT).

1. **Antiterrorism.** Defensive measures used to defend against and/or defeat terrorist strikes. These measures can include, but are not limited to, physical security devices such as barriers, fences, guard forces, access controls, surveillance systems, and security education. In the Office of Security, responsibility for implementing antiterrorism policies and procedures rests with the Physical Security Program.

2. **Counterterrorism.** Proactive measures that are taken to defeat terrorists and prevent an act of terrorism before it is committed. Inquiries or investigations, threat analysis, and threat alerting mechanisms are included. In the Office of Security, responsibility for implementing counter-terrorism policies and support rests with the CI Program Branch.

C. The CI Program Branch threat analysis will be an ongoing effort to identify potential terrorist interest in departmental persons, facilities, information, or activities.

D. The CI Program Branch will establish and maintain an effective liaison program with the Federal counterterrorism community to include representing the Department at community boards, committees, working groups, and task forces. The CI Program Branch will ensure the timely receipt and dissemination of pertinent information and intelligence to departmental recipients.

4215 Counterintelligence Support to Departmental Activities

A. The DCIP supports all departmental activities. Operating unit security contacts and servicing security officers should identify functions, missions, and activities that could be candidates for CI

support. Together the CI Program Branch and the servicing security officer concerned will review this information and determine the nature and extent of CI support.

B. From time-to-time, the Department's activities and programs may come under the scrutiny of a foreign intelligence service. In such cases, any one of the activities or programs will benefit greatly from having a previously completed CI assessment.

4216 Counterintelligence Activities in the Operating Units

A. In the Department, the counterintelligence function has been centralized in the Office of Security. CI personnel are not assigned to the operating units, nor are they assigned to regional or field security offices. The CI Program Branch serves as both the CI policy office as well as the Department's CI investigative element. This is not, however, at the exclusion of the operating units. Issues and incidents mandating CI involvement occur in the operating units. Servicing security officers implement the DCIP, in part, in their respective areas of responsibility.

B. The core issues of CI concern must be an integral part of the routine security curriculum at each of the operating units. These core issues are:

1. FIS activity;

2. Economic espionage;

3. Employee education and awareness;

4. Illicit technology theft/transfer; and

5. Terrorist interest and/or targeting.

C. Generally, identification of issues # 1 through # 4 and implementation of issue # 5 will be accomplished by Office of Security servicing security officers and by operating unit security contacts. Resolutions of issues # 1 through # 4 and product support for issue # 5 fall under the purview of the CI Program Branch.

D. If servicing security officers or security contacts learn of any information regarding issue B.1. through B.5. above, they should contact the CIPB immediately in order to obtain additional procedural guidance.

E. Servicing security officers or security contacts must conduct internal CI awareness training, utilizing approved materials. Contact the CI Program Branch for assistance.

F. The CI Program Branch is available to conduct a CI needs-assessment on any activity to assist a servicing security officer or a security contact in defining the CI needs of their organization.